future identity

INDUSTRY INSIGHT

# Biometrics for business

Real-world use cases, from the businesses deploying face biometrics to solve identity challenges.

Powered by:

proov

# Identity in a Digital Age

**The rate of change for businesses in the current digital age is immense. Dozens of new technological solutions and products hit the market every month, offering to help enterprises meet consumer expectations and stay competitive.**

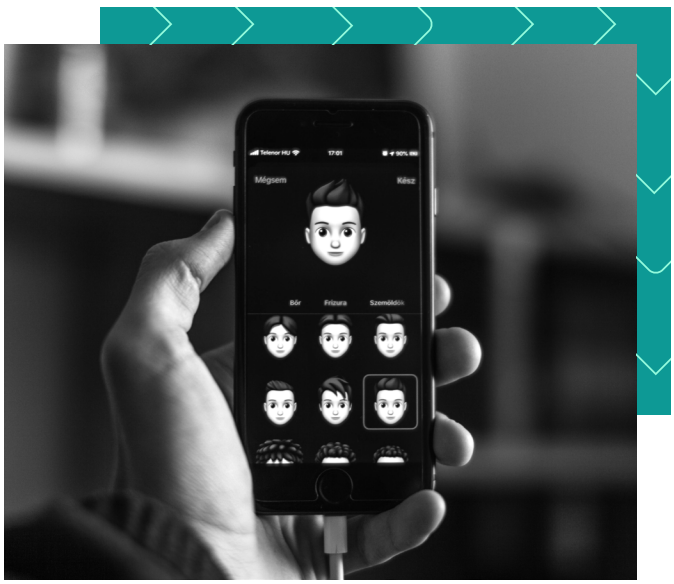
When it comes to knowing a customer's identity, many businesses are responding to digital demand by incorporating verification and authentication into their online channels. Yet in order to keep up with a rise in sophisticated cyber-attacks, increasingly robust digital security measures are required.

**Traditional methods of managing identity, such as passwords, secret answers and SMS codes are simply failing to keep pace.**

The COVID-19 pandemic only accelerated the digital shift. Social distancing and stay at home orders intensified the need to allow employees and customers to work and transact remotely. Businesses reliant on in-person interactions to verify identity, were forced to consider how verification could be managed online.

With the vaccination rollout underway, many countries are beginning to emerge from the worst phase of the pandemic. As society transitions back to normality, or what many are referring to as the 'new-normal', the use of digital services will remain part of our everyday lives.

Trusted identity technologies have become an essential element of any enterprise's digital strategy.




**Organisations across all industries, will need solutions in place to provide robust security against a growing set of threats, as well as a frictionless online experience.**

Increasingly organisations are turning to biometrics in order to meet this challenge.

# The Power of Biometrics

**Biometric technology has been in use for decades in many different scenarios, from law enforcement to access security. Now a growing number of consumer-facing businesses are also turning to biometrics, as part of their digital identity strategy.**

**When compared with traditional knowledge-based methods of identification, biometrics offer far higher levels of assurance and convenience.**

Security questions can be a frustrating barrier for customers attempting to access their accounts or data, while the majority of passwords are not secure and are easy for customers to forget, or fraudsters to capture.

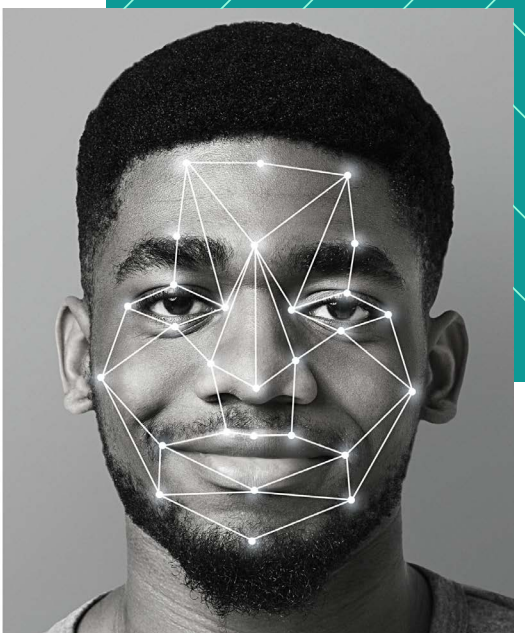
When a business does not fully ensure that a customer's identity is genuine, fraudsters are given the opportunity to cause financial and reputational havoc. In just minutes, an imposter can drain a customer's account, leading to a loss of customer trust, often heavy fines from regulators and adverse media attention.

The power of biometrics for identity verification lies in their uniqueness to each individual, making them extremely difficult to replicate.

**A face biometric is particularly powerful, as when combined with a scan of a government-issued ID document, it can be used to securely bind a digitally presenting individual to their legal identity.**

Increasingly this method of establishing trust is used to onboard customers digitally, not only a substitute when in-person interaction is not possible, but as a preferred option.

The eIDAS regulation in Europe, for example, attests to the strength of face biometrics – permitting their use, alongside a document verification, to enable a qualified signature to be created remotely.

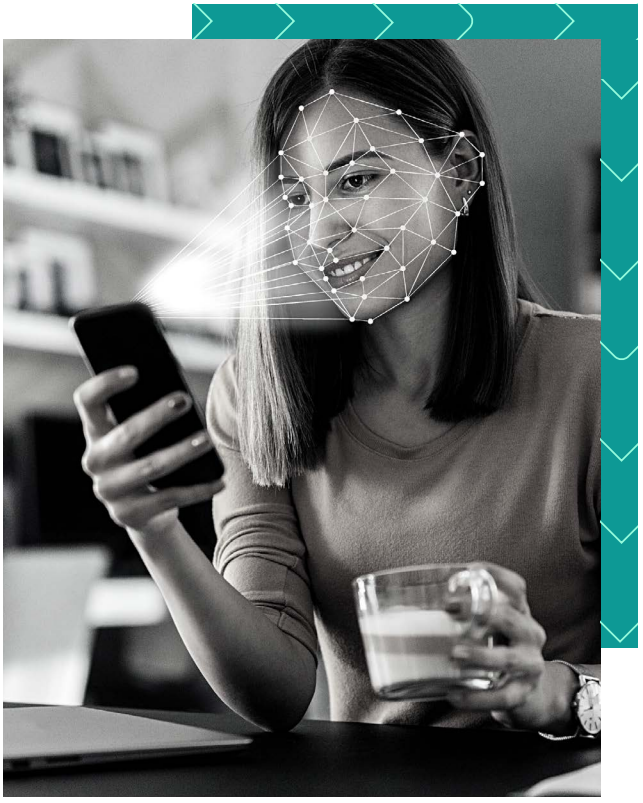


**In today's always on, always connected society, convenience is key.**

If a potential customer is confronted with a verification process requiring them to bring documents to a physical location or fill out excessive amounts of data on multiple online forms, they are likely to get frustrated. They may abandon enrollment or be left with a bad impression of the company.

As a business grows and sees increasing numbers of customers signing up to use their products or services, a cumbersome onboarding process can become a bottleneck for scalability.

**Providing the option of remote onboarding and ensuring verification processes are as fast and smooth as possible, is key to ensuring high completion rates and increased customer acquisition.**



Face verification offers an ease-of-use, capable of meeting this demand for convenience. What's more, once a secure digital credential is created at enrollment, it becomes possible for customers to carry out secure re-authentication with just a simple face scan. The user won't be required to re-enroll each time they access a new service and the business will benefit from simplified due diligence and reduced risk when making updates to a customer's profile.

This much sought-after balance of convenience and security might sound too good to be true, but biometric technology is already delivering on its promise in many real-world business use cases.

# Biometrics in Practice

**The COVID era undoubtedly introduced a number of new challenges for businesses. The long-term impacts of the past year on the future of work will be profound, with many enterprises maintaining remote working, learning, banking and shopping as a core offering moving forward.**

Biometrics could play a key role in enabling this shift. Long before the pandemic, companies in many industries had already successfully deployed facial biometrics for verifying customer identity. From governments and airports to banks and hotels, a diverse range of enterprises in a variety of sectors are finding that biometrics offer immense value.

## Margo Stephen

Head of Digital iD,
Identity Payments
and Financial Services

AUSTRALIA POST

### How did you decide that face biometrics was the best route to solving the challenge of verifying and authenticating customers in a digital world?

We considered the different levels of assurance that exist within Australia, outlined by the government's Trusted Digital Identity Framework. We wanted a solution that would achieve a range of assurance levels. Biometrics enabled high assurance without in-person interaction. Effectively we wanted to complement our existing in-store services with digital equivalents for the online world.

We knew that face biometrics would enable comparison between identity documents and the individual presenting them, giving us the right balance of assurance and enabling a virtually 'frictionless' onboarding process. The idea was for customers to go through a little bit of friction initially in order to create a reusable digital identity for future lower friction transactions.

### What are some of the operational use cases and outcomes to come from your use of face biometrics?

We incorporated biometrics into the app used by our customers who choose to create a reusable digital identity. Information is extracted from a customer's passport using the NFC reader on their mobile device and is compared to a selfie and liveness detection scan. The biometric bind with a verified document creates a strong digital identity, which an individual can use to prove their identity to relying parties or in-person to other individuals with a Digital iD.

The key word for our approach is 'ecosystem'. We want to make sure lots of individuals have a digital identity, but also that there are lots of places where they can use it. Much of our work has been collaborating with a wide range of organisations across the public and private sector to enable them to connect to our services. Interoperability is hugely important.

> **"We want to make sure lots of individuals have a digital identity, but also that there are lots of places where they can use it."**

### Which inclusivity factors were considered when deciding on an appropriate biometric solution?

The vast majority of Australians have the technology and documentation needed to create an identity digitally. But there is a group of people left behind. Not every customer has a phone capable of downloading and running our app, there are also demographics from remote/rural communities to consider, or those without documentation - which can be for any number of reasons, including those fleeing domestic violence who have been forced to leave their documents behind.

This group may be a minority, but it is still critical that we enable them to create a reusable digital identity. So if customers cannot onboard digitally or don't have a passport which can be electronically verified, they can bring a broader set of documents to an Australia Post branch to be verified in-person.

It's also very important to follow web accessibility standards wherever possible for any application we build. Australia Post is an organisation for everyone.

> **It is important to build trust by ensuring consent is extremely explicit at all steps in our process.**

### How did your customers respond to using biometrics?

As more and more services transfer online, particularly given the impact of COVID, we are seeing a greater uptake of digital in general. There is more acceptance of using apps, scanning QR codes and interacting digitally and people are less concerned about technologies like face biometrics than previously.

It is important to build trust by ensuring consent is extremely explicit at all steps in our process. It has recently come to light that some social media apps collect face or voice biometrics from their users, which shows how often users accept terms and conditions without considering the potential long-term consequences. For us, transparency about where information (including biometrics) us being used, is essential.

> **In order for biometrics to fully take off people need to be confident about the benefits and be assured of where their information is going and what it can and can't be used for.**

### Do you think that the use of biometrics will become the norm for businesses in the future?

I think it will. People are becoming more comfortable with the technology, so it's only a matter of time. In order for biometrics to fully take off people need to be confident about the benefits and be assured of where their information is going and what it can and can't be used for.

It can take a long time for a customer base to fully trust a new technology - look at the number of years it took chip and PIN to become widely adopted in the UK for example. That being said, COVID has accelerated the number of online transactions and made people think differently about how they interact with technology. I think this could certainly reduce the change period required for biometrics to become the norm, we just have to make sure services are accessible and inclusive so no one is left behind.

## Rod Boothby

Global Head of Identity

SANTANDER

### Can you outline some of the challenges your organisation faces, onboarding and authenticating customers in an increasingly digital world?

Digital onboarding is a huge challenge for us globally. Local regulation has an impact on the solutions and technologies we can use in different locations. In Mexico for example, a live video chat with a human is required to review account applications. Then there are also several countries where digital onboarding is prohibited.

Overall, authentication is best managed by dynamically assessing the risks associated with digital and adjusting to bring in, where necessary, a range of step-up capabilities. These might include device authentication, network characteristics and data, locally installed cryptography, or where possible using local code running in a secure enclave to obtain biometric measurements to compare with server-side information. Independent facial recognition, voice recognition, fingerprint and thumb print recognition can also be key, as can bot detection, liveness testing, and shared secrets.

> **"If implemented well, face biometrics can increase customer satisfaction and result in fewer calls to our call centre."**

### How has implementing face biometrics helped to address these challenges?

Our goal is to create a multi-channel, multi-dimensional assessment of whether the person at the end of a specific digital session, is the same human we got to know during onboarding.

Face biometrics is one piece in that puzzle. It's powerful, but not perfect. Then, no one technology is.

### How did your colleagues and customers respond to using biometrics?

If implemented well, face biometrics can increase customer satisfaction and result in fewer calls to our call centre. We don't use face biometrics everywhere. There have been a range of reactions, depending upon the specific technology, the use case and the range of equipment used by the customer base.

### Which inclusivity factors were considered when deciding on an appropriate biometric solution?

We select technology that helps us to make sure all our customers and employees feel valued and respected. We have to remember that not everyone has the latest device. We must provide solutions that work for everyone.

### Do you think that the use of biometrics will become the norm for businesses in the future?

Biometrics will be used, but I think that the majority of people will want to limit the number of partners they share their biometrics with. This is one of the reasons why we are working on a Bank ID Verification solution. Customers will be able to prove who they are without feeling they are over sharing sensitive biometric information.

## John Skipper

Chief Information Security Officer

METRO BANK

### What are some of the challenges organisations face onboarding and authenticating customers in an increasingly digital world?

We constantly have to consider the balance of usability against security. If you try to make things too secure you start to impact usability, but if you make things too quick and convenient it won't be secure enough. This is starting to become a well understood art, we know roughly where the middle ground is, as do the technology partners we work with.

> **We constantly have to consider the balance of usability against security.**

### Can you outline the operational use cases to come from your use of face biometrics?

For the purposes of new account opening, we use facial comparison to validate a user's appearance against the photo on their passport or driving licence. Our solution provider is able to check physical security features to assess whether the document presented is genuine.

The user is then required to capture a single high quality 'selfie' frame, as well as a short video where elements of liveness detection look for eye movements, or the motion of breathing. The result is a reasonably high level of confidence in the genuine identity of the user and the validity of the physical document backing up this identity.

### In future are you looking to expand your use of face biometrics to other use-cases?

Currently, customers can access credentials or authorise high-risk payments on their mobile device with fingerprint recognition, using the built-in biometric capabilities on Android or IOS. Employees use the same technology, rather than entering their email address and a secure password, which can be a real pain on a mobile keypad.

Whether we expand our use of face recognition to cover authentication as well, would really depend on the phone manufacturers. Apps such as Windows Hello, which use a phone or laptop camera for face recognition, give a high-quality of log-on confidence but tend to require a high-spec device.

This would only really work for our employees, or potentially corporate customers. Personal banking customers should have an equally seamless experience with online banking, no matter which browser, device or operating system they use.

> **Personal banking customers should have an equally seamless experience with online banking, no matter which browser, device or operating system they use.**

> **Biometrics allow us to reach the necessary hygiene level for fraud control with much less impact on usability.**

### How has the use of biometrics helped you to address your identity challenges?

Biometrics allow us to reach the necessary hygiene level for fraud control with much less impact on usability. The technology improves the security around re-entry of credentials, as there is far less risk of accidentally entering your biometric in the wrong place or giving it away. It is much harder for someone to lift it and steal it compared to a password. Overall, Biometrics are a bit more secure, but a lot more convenient.

### How did customers respond to the use of biometrics?

Our onboarding solution is very user friendly. There are cases where the user's photo is not high enough quality and they are asked to take it again, or occasionally are not able to onboard with this method. But overall, users are used to the process now and so for the vast majority of customers it works very well.

We can offer much more convenient services online than we can in-person (although we do still offer a full service in our branches). Allowing people to sign up for internet and mobile channels whenever they need them, and as quickly as possible has been very important. Lockdown made this even more vital, as online was the only place customers were able to open an account.

### Do you think that the use of biometrics will become the norm for businesses in the future?

Yes. It is happening, although perhaps more slowly than previously expected. Biometrics aren't perfect, they have their risks and benefits, with different biometrics having different levels of convenience and security.

In terms of the number of false positives you can tune for, biometrics is not vastly more secure, but password compromise has become an extremely significant problem. If a customer were to ignore advice and use the same password with our app as they do for other important services, a compromised password would mean all accounts are potentially compromised.

As a whole, biometrics are now sophisticated enough to provide slightly better security and much better usability.

> **Allowing people to sign up for internet and mobile channels whenever they need them, and as quickly as possible has been very important.**

## Margus Arm

Deputy Director General

ESTONIAN INFORMATION SYSTEM AUTHORITY

**Estonia has a well-established digital identity ecosystem. Can you elaborate on the types of eID citizens have access to?**

In Estonia, we have three different eID solutions. The first is a PKI and chip-based ID card, issued by the government's Police and Border Guard Board. Secondly, citizens can get a SIM and and PKI based mobile ID, obtained from the mobile network operator. Finally, there is the option to use Smart ID, which is a mobile application available on smartphones and tablets. All three forms of digital ID are linked and can be used interchangeably to authenticate identity or provide a digital signature online.

**How have you incorporated face biometrics into the digital ID program?**

Currently, face-to-face verification is required to apply for the ID card, which is a mandatory document for citizens aged 15 and above. This can be done in the offices of the Police and Border Guard Board, all over the country. Mobile ID can be set up after having received a relevant SIM card from the mobile network operator. To set up the Smart ID, citizens can download the app and activate it using their existing ID card or Mobile ID, or alternatively can go to the bank to complete a face-to-face verification.

In a fairly recent development, users wanting to renew their Smart ID can now do so remotely using face authentication. Using the Smart ID app, users scan their passport chip and take a selfie, then iProov will compare the data and give a confirmation as to whether the identity is a match.

> **As a government, we have to thoroughly mitigate risk and cannot accept even a minor margin of error when it comes to verifying identity.**

**How will you continue to adapt to an increasingly digital world, especially given the impact of pandemic over the past year?**

During the pandemic, our ability to offer three different identity tokens was critical in ensuring citizens were not so badly impacted. When the mobile network operators closed their shops for example, at least one other form of digital ID still remained accessible.

We are always considering new and improved enrollment processes to provide more convenient services. However, it is important to weigh up whether the inconvenience of physical face-to-face verification once every 5 years when an ID card expires, is enough to justify the additional complications and risks of enabling fully remote onboarding. As a government, we have to thoroughly mitigate risk and cannot accept even a minor margin of error when it comes to verifying identity.

> **Users wanting to renew their Smart ID can now do so remotely using face authentication.**

> Estonia is a heavily digitized society. Many people want to use nothing but the latest devices and technological solutions. However, with three different forms of digital ID available, there is something for everyone.

**98% of Estonian citizens use digital identity, how do you ensure the system is so inclusive?**

Estonia is a heavily digitized society. Digital ID was introduced back in 2002, so by now people are very used to accessing state services online and using the digital signature. After close to 20 years of building up a digital government, many people want to use nothing but the latest devices and technological solutions.

However, with three different forms of digital ID available there is something for everyone to feel comfortable with. Those without a mobile device can use their ID card inserted into their laptop or PC, those with an older SIM-based mobile rather than a smartphone can use the Mobile ID. Then if you are technologically advanced you can use the smart ID. The government also continuously provides people with free software to use the digital signature.

**Do you think biometrics will become the norm for many businesses and services in future?**

Yes, I think the technology is already on the market and is getting better and better every day. People find biometrics very easy to use, they can take a selfie and get immediate access to accounts or transactions, which is extremely convenient. We need to ensure however, that we fully understand and manage the risks associated with biometrics, such as deep fakes, so that we truly know who is in front of the phone. Biometrics will provide an additional level of security to existing identity solutions.

# Biometrics for everyone

**Responsible businesses are increasingly turning their attention to digital inclusion. Ensuring digital solutions fit to a wider accessibility framework, allows organisations to better meet the requirements of their customer base.**

**Biometric solutions should be designed to provide effective identity verification for everyone, regardless of ethnicity, gender, economic circumstance, disability or age.**

Solutions must be designed and algorithms trained, to mitigate bias. Rigorous performance testing is essential to ensure mitigation is successful.

While the vast majority of people will be able to use face biometrics, some may experience challenges. Those with disabilities such as visual impairment for example, may struggle if a solution requires them to position their smartphone at a certain angle.

Of course, each type of biometrics will present unique challenges to different groups. Those with a voice tremor, may struggle with voice authentication, while individuals with mobility problems may not be able to use fingerprint verification.

There are also circumstances which may prevent non-disabled individuals from effectively using biometrics. A customer may not always be in a situation where it is appropriate to speak in order to use voice authentication, for example.

Those who regularly do manual labor may struggle to use fingerprint biometrics and not everyone is comfortable seeing themselves on camera in order to use face biometrics.

Face verification needs to be able to be used by customers of all ages and technical abilities. This means clearly guiding users through the process – even those with hearing or visual impairments - and reassuring them of any concerns regarding the technology.

**Ensuring the solution is usable on any device, removes prejudice against those without the latest smartphones and allows businesses to be inclusive of customers no matter their economic situation.**

Focusing on usability will allow enterprises to take advantage of the benefits of face biometrics, without excluding marginalized groups.

## Andrew Bud

Chief Executive Officer

IPROOV

**Organisations today face various challenges when it comes to verifying and authenticating users online. What makes biometrics so effective at addressing these challenges?**

Firstly, security. Biometric technology today offers the very highest levels of online security with effortless usability. For a bank, for example, online biometric authentication is so secure that customers can complete processes such as changing a PIN, requesting a new debit card or transferring a large amount of money, all with a simple face scan. These things used to require a lot of checks and a lot of effort from a customer. Biometrics is changing the way that banks, governments and other security-conscious organizations deliver digital services.

Secondly, usability. A passive biometric authentication solution requires no effort from the user at all. Just compare the experience of taking a few seconds to complete a brief face scan with the frustration of trying to request a password reminder. Biometrics is the way forward for organizations that want to build trust with their customers without compromising on security or simplicity.

> **"Biometrics is the way forward for organizations that want to build trust with their customers without compromising on security or simplicity."**

> **"70% of Americans and 69% of people in the UK either use Face ID to access their mobile banking app already - or would do so if their device supported it."**

**How are consumers responding to the increased use of this biometrics?**

Biometrics are becoming ubiquitous. Consumers are now very comfortable with using their faces or fingerprints to unlock their phones and access their mobile apps. We did some research recently that showed 70% of Americans and 69% of people in the UK either use Face ID to access their mobile banking app already - or would do so if their device supported it.

Like any on-device biometric solution, Face ID has its limitations in terms of security but it proves beyond doubt that consumers are very happy to authenticate using their face. There's a huge opportunity for banks to capitalize on that by implementing secure cloud-based biometric technology so they can reduce costs and fraud, while offering an extremely convenient service.

**How are organizations using biometric authentication today?**

iProov delivered the world's most successful remote identity verification immigration program with our partners, WorldReach. Together we processed 5 million applications for the UK Home Office's EU Settlement Scheme. Applicants were able to complete the application in under 10 minutes, with a high level of identity assurance.

Rabobank (one of the top 50 banks worldwide) uses iProov within their mobile onboarding app to allow 18-year-old customers to upgrade to an adult account. This ensures that the customer does not need to visit a branch for in-person verification. As a result, Rabobank saw its mobile channel share grow from 35% to 60% for this customer segment within one year.

### What should organizations take into consideration when choosing a biometric solution?

It's vital to take a customer- centric approach. You must consider inclusivity - it's no longer acceptable to assume that your users can or want to follow instructions. Consider the cognitive ability of the user. Can the user authenticate themselves effortlessly, with no audio or written instructions?

There should be no prejudice around devices either. For example, the app that the UK Home Office created for their EU Settlement Scheme has been accessed by more than 2300 different devices. So, you must be inclusive across brands, platforms and even the age of the device.

For the Singapore Government's SingPass digital identity solution, bias monitoring was key.  SingPass provides 4m Singapore residents with secure access to over 500 public and private digital services. Any face authentication had to cater for their diverse ethnic population.

> **You must consider inclusivity - it's no longer acceptable to assume that your users can or want to follow instructions.**

> **The pandemic has forced consumers and businesses into increased online interaction. This has led to a huge rise in attempted fraud.**

### Do you think that the use of biometrics will become the norm for businesses in the future?

The pandemic has forced consumers and businesses into increased online interaction. This has led to a huge rise in attempted fraud and manipulation of customer information, which in turn has led businesses to move away from knowledge and possession-based authentication methods. We will continue to see the growing use of biometric authentication, from opening a bank account remotely to proving your COVID Status Credentials (CSC) when travelling.

# Looking to the Future

It's clear many businesses are ready to invest in a digital future where customer verification is both secure and seamless. For customers, onboarding to and accessing online services will be increasingly easy as biometric solutions become commonplace. Businesses, too, will benefit from reducing the manual workload placed on employees to check identity documents, combating fraud and more efficiently meeting regulation.

Like any other digital transformation, incorporating face biometrics into an enterprise's operations will not be without its challenges. But once set-up, the technology has the potential to deliver streamlined and cost-efficient processes, across a wide range of industries.

As one of the fastest-growing global technologies, the use of face biometrics looks set to become an integral element of many businesses' future digital strategies.

future identity

# ABOUT IPROOV

iProov is the world leader in using biometric face authentication to confirm that an individual is genuinely present during an online interaction. iProov's Genuine Presence Assurance technology is used by governments, banks and other enterprises globally to verify that a user on a mobile device, computer or unsupervised kiosk is the right person, a real person, and, critically, that they are authenticating right now – not a digitally injected attack using deepfakes or other synthetic media. Established in 2012, iProov is headquartered in London with offices in Maryland and Singapore.


## Andrew Bud

Chief Executive Officer

iProov

Email: contact@iproov.com
Website: iproov.com

## Laura Camplisson

Future Identity Portfolio Lead

VC Innovations

Email: laura.camplisson@vcinnovations.co.uk
Website: thefutureidentity.com